Declaration
of
Ron Schnell

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

DECLARATION OF RON SCHNELL

BERNADINE GRIFFITH, ET AL.

V.

TIKTOK INC. AND BYTEDANCE INC.

CASE NO. 5:23-CV-00964-SB-E
UNITED STATES DISTRICT COURT FOR THE CENTRAL DISTRICT OF CALIFORNIA

JULY 12, 2024

TABLE OF CONTENTS

I. EDUCATION AND EXPERIENCE

1. I am a Managing Director at Berkeley Research Group, LLC ("BRG"), which is a global consulting firm that helps leading organizations advance in three key areas: disputes and investigations, corporate finance, and performance improvement and advisory. I have over 40 years of experience in the fields of computer science and software. I have a master's degree in computer science from Syracuse University and have a working knowledge of over 40 computer languages, including all of those at issue in this matter.

2. I specialize in analyzing and enabling network traffic and have written many of the major network device drivers in use for the UNIX operating system and variants.

3. My curriculum vitae, which reflects a subset of my work experience, is attached as Appendix A to this report. Appendix B includes a list of cases in which I have testified either at deposition, trial, an evidentiary hearing, or a live arbitration within at least the last four years. I have highlighted some of my work history below.

4. Over the course of my career, I have worked at many of the world's largest computing companies, including (but not limited to) Bell Laboratories, IBM Corporation, and Sun Microsystems. I was also an early researcher on the Arpanet, which later became the Internet. In addition to working at large corporations, I have founded three start-up companies to date, including a backup and restore software company and a .COM company which I sold to a public corporation in 2000.

5. Early in my career, I worked at the Artificial Intelligence Lab at the Massachusetts Institute of Technology. Later, in approximately 1986, I worked at Bell Laboratories on the UNIX

Operating System, writing many thousands of lines of source code representing portions of the core kernel of the UNIX operating system.

6. From 1988 to 1990, I worked at IBM Corporation on their operating system called AIX (for the IBM 370 mainframe, as well as the IBM PS/2), functioning as a programmer, and eventually a development manager. From 2002 to 2005, I was a Vice President at Equifax Corporation, one of the three major credit bureaus in the United States, leading software development in their Internet Marketing division. In this role, I was responsible for all of the software (including web software) that was used for marketing on the Internet. I was responsible for all web-based consumer information collection, including using pixels and web-based APIs.

7. I have also been on staff and consulted at numerous other companies and institutions, including (but not limited to) Syracuse University, Encore Computing Corporation, Harris Computer Corporation, and ITT. I am currently an adjunct professor of computer science and was previously an advisory board member at the College of Engineering and Information Science at Nova Southeastern University.

8. From 2005 through 2011, I was responsible for monitoring Microsoft Corporation in connection with the antitrust litigations brought by the U.S. Department of Justice and the Attorneys General of 19 states in *United States v. Microsoft* and *New York v. Microsoft*, Civil Action No. 98-1232 (TPJ), Civil Action No. 98-1233 (TPJ), (D.C. Cir.). In this role, I had responsibilities akin to those of a Special Master, and provided periodic compliance reports to Hon. Colleen Kollar-Kotelly of the United States District Court for the District of Columbia. I was responsible for directing the day-to-day enforcement of the final judgments against Microsoft, and supervised a team of 93 people in performing these duties.

9. I have managed software projects of all sizes, from custom-built software for hire to software programs that have hundreds of millions of users, and I have managed programming teams from as small as one programmer to over one hundred programmers.

10. Two publications I have written in the field are: Jay L. Himes, Jason Nieh & Ron Schnell, *Antitrust Enforcement and Big Tech: After the Remedy Is Ordered*, 1 Stanford Computational Antitrust 64 (2021), and Ron Schnell, *Hacking 101: Using Social Engineering Increases Security Attack Effectiveness*, Coast Guard J. of Safety & Sec. at Sea, Procs. of the Marine Safety & Sec. Council 71, no. 4 (2014) 25–27.

II. RETENTION IN THIS MATTER

11. I have been retained by Counsel for Defendants TikTok, Inc. ("TTI") and ByteDance, Inc. (collectively, "Defendants") to serve as an expert witness in the field of computer science, computer software, software development, computer privacy and personal information tracking in the above-captioned action. BRG is compensated for my work in this matter at the rate of $950 per hour. My compensation is not contingent on the outcome of this case.

12. I have been asked to explain about the functionality of certain software tools, what information they collect, the functionality of the "TikTok Pixel", "Events API" ("EAPI"), and data analytics.

13. I have also been asked to opine in rebuttal to the Declaration and Expert Report of Dr. Zubair Shafiq in Support of Plaintiffs' Motion for Class Certification (the "Shafiq Report") and, where applicable, the Declaration and Expert Report of Russell W. Mangum III, PhD (the "Mangum Report"), both filed with the Court on June 21, 2024.

14. All of my opinions are based on a reasonable degree of scientific certainty in my field of computer science.

III. MATERIALS RELIED UPON

15. The materials I relied upon in forming my opinions are identified in Appendix C.

16. To the extent that I obtain additional information subsequent to this Report that requires me to amend or expand my opinions, I reserve the right to do so via a supplemental or amended report.

IV. SUMMARY OF OPINIONS

17. **TTI provides two tools to advertisers: the TikTok Pixel and the TikTok Events API ("EAPI").** These tools are markedly different in the way that the technology works, and require different analyses in terms of what data they transmit, and when. [redacted] Only advertisers can ensure these tools are used correctly.

18. **Whether and what data are disclosed to TTI via the TikTok Pixel or EAPI requires an examination of individual circumstances.** There are many factors that determine which data are transmitted via these tools, and these factors can be different for each person who visits the advertisers' sites, as well as for each advertiser's site. [redacted]

[redacted]

19. **Whether or not "search terms" or any specific website user communications were transmitted to TTI requires an examination of individual circumstances.** As discussed by Dr. Shafiq, [redacted] It is dependent on the functionality of the advertiser website, as well as the way it is designed. Advertisers have control over data that are transmitted as part of the URL, not only to TTI, but over the Internet in general.

20. **Whether [redacted] or sensitive information was disclosed requires an examination of individual circumstances.** Dr. Shafiq opines on [redacted][1] [redacted]

21. **Whether "contents" of a communications by a website visitor are transmitted while "in transit" to that website requires an examination of individual circumstances.** Some data transmissions depend on what each user actually does on the website, and how that affects the timing of transmissions. This timing is also different when comparing the TikTok Pixel and EAPI. A full understanding of the way the Internet and the World Wide Web shows that browsing information is not consistently transmitted to TTI while it is in transit, in any case.

[1] Shafiq Report ¶ 63(v).

22. **Data collected through Google Ipsos is not comparable to data collected via the TikTok Pixel, and even more so via EAPI.** Google Ipsos collects data about websites visited by its panel members, as well as their interactions on those websites and other devices, like cellphones. Additionally, Ipsos collects data from non-website activity by its panel members. It is a comprehensive Internet tracking tool that also includes the identity of the panel members. The TTI advertiser tools are substantially limited, compared to Google Ipsos. The "seven data categories" that Dr. Shafiq discusses at length in the Shafiq Report and his deposition are a small subset of the data collected by Google Ipsos.

V. TECHNICAL BACKGROUND

23. The "World Wide Web" and Web Browsers were created as a way to allow Internet users to visit pages of information. In the early days of the Internet, consumer network connections were very unreliable, mostly due to the use of dial-up—a method of connecting to the Internet through public telephone networks. Therefore, it was thought to be important that web browsing be *stateless*. This means that a user's browser would not have to store any particular information about the web pages it visited. One could go to a website, navigate around, go for lunch and come back again, and continue browsing. Web pages were written so that each time information was requested, it was as if it was from a new person, and it would never rely on any sort of continuity.

24. As time went on, and the obvious desire developed for websites to become personalized, different methods of maintaining *state* were used. These methods included HTTP Authentication, Query String CGI, and eventually cookies. Cookies were a distinct departure from the way browsers were intended to work. They created *stateful* browsing, where the browser stored information that could be passed back and forth between the browser and the website.

25. In order to maintain privacy, the inventors of cookies and the browser manufacturers took care to make sure that cookies could not be shared between companies. When a website wants to use cookies, there is special source code on the page that tells the browser that it will be storing a cookie. This cookie can contain any information the website desires. It can be something simple like a bookmark, so that the next time that browser goes to the page it can start where it left off. Or it can be much more complicated, storing all sorts of preferences.

26. Importantly, what is stored in the cookie itself is stored in the users' browsers, and not the website itself. Therefore, the most common use of a cookie is to store a very small amount of data. These data are typically a unique identifier that ties to the *real* data, which is stored on the database of the website. For example, a website might store a cookie in your browser called "PREFERENCES" that contains nothing but the number "00000121241". Somewhere in a database on the website's server, there is a mapping of the number 00000121241 to things such as your language preference, your time zone, etc., so that the next time you visit the website it remembers those things. In this scenario, the number 00000121241 is not useful to an ordinary person who does not work for the website's company.

27. Additionally, there is no *technical* difference between "first-party" cookies and "third-party" cookies. There is really only one type of cookie. **All** cookies can only be set and read by the same website (domain), i.e., only the domain that sets the cookie can read it. Cookies are called "third-party" under the circumstance when a website visitor arrives at a webpage with a pixel installed, the user's browser then visits a different website, and that later website has a previous cookie that is set on the user's browser, in which case that website can retrieve it. This is most useful if the user visiting the first website has a previous relationship with the second website.

28. Pixels were also added to the World Wide Web later on in its development. Early web pages were "static", in that they contained information that could not change. For example, websites were created to show weather forecasts or news articles. The text of the webpage was set up on the website, and when a user visited the webpage, they would see the text, e.g., the weather forecast for tomorrow.

29. But it soon became desirable that the server itself be able to change the output of the webpage dynamically. The way this was done was to make it so that when a webpage had an *image* on it, that image could cause actual programs to be run by the server. The server would then do whatever it wanted, and then vary the output in the form of an image that a web visitor would see.

30. This was revolutionary to the World Wide Web, in that webpages could be dynamic. It was not long before this functionality was utilized by advertisers and marketers. By having images that are ultra-tiny (e.g., a single pixel), there would be nothing noticeable displayed to the web visitor, but the server in the background could take note of things that were useful in marketing, such as clickthrough rate, open rate, and conversion rate.

31. With the advent of rich client-side languages such as JavaScript and server-side frameworks, the original use for image-based server-side scripting was no longer necessary, and today this functionality is almost exclusively used for marketing and advertising.

32. In this report and in the Shafiq Report, when the TikTok Pixel is discussed, we are talking about a pixel-sized image referenced on advertisers' webpages that is hosted by TTI, and thus cause communication between the advertisers' websites' visitors and TTI.

33. When images (including pixels) are seen by the browser, it makes a separate communication with the site that hosts the images (such as TTI). All communications over the World Wide Web contain a certain minimum amount of information, simply because of the way the Internet and the HTTPS protocol functions. These include: a timestamp, an IP address, a User Agent, Cookies, and certain URLs. In other words, this information is delivered to *every website every user ever visits*.[2]

34. Online users' browsers communicate data to a website, whether it is the first visit or when going from one page of a website to another, via an object called a "form". For example, if a user performs a search on a search engine, the user types search terms into a form and presses the enter key or clicks on the search button.[3] This is called entering parameters into a form. The form object typically sends the browser to a different page on the same website and passes the search term parameters (and perhaps other parameters) to the other page. There are two standard methods of doing this: GET and POST.

35. The GET method simply adds the parameters to the end of the URL, so the receiving webpage need only look at the incoming URL to get the parameters and perform the search. The early World Wide Web *only* had the GET method, and developers had no choice but to put all of the parameters in the URL.

36. The following version of HTTP (in 1996) introduced the POST method. This was very important for privacy. It allowed webpages to communicate parameters to other pages

---

[2] An exception to this is if a browser has a "cookie blocker", in which case cookies will not be sent.

[3] In the modern web, there are ways other than users actually typing into a form to create parameters. This is simplified for brevity.

without putting them in the URL. This meant that the parameters could not be seen by the website visitors themselves, or if other websites were able to see the URL, it would *not* see the parameters.

37. The POST method immediately became best practice for any website that did not want to share parameters with anyone who could see the URL, and still is best practice today.[4]

VI. TTI PROVIDES TWO TOOLS TO ADVERTISERS

38. TTI provides two different tools to advertisers: TikTok Pixel and the TikTok Events API. They are markedly different in the way they operate, and must be analyzed separately from each other.

A. TikTok Pixel

39. TikTok Pixel is JavaScript code that must be embedded into the advertisers' websites in order to work.[5] The JavaScript code runs on the users' browsers, and not the website's

[4]See Kevin Beaver, *Why use POST vs. GET to keep applications secure*, TechTarget (Feb. 9, 2010), https://www.techtarget.com/searchsoftwarequality/tip/Why-use-POST-vs-GET-to-keep-applications-secure ("… is the POST method better than the GET method for processing HTTP requests? The common response is always use POST. Problem solved. Security breaches in recent years involving mishandled and unsecured information between the browser and the server have helped to underscore this importance." … "With GET requests, there are numerous ways for sensitive information to be exposed"); W3Schools, *HTTP Request Methods* (2024),https://www.w3schools.com/tags/ref_httpmethods.asp ("GET is less secure compared to POST because data sent is part of the URL. Never use GET when sending passwords or other sensitive information!"); Janlori Goldman, Zoe Hudson, and Richard M. Smith, *Privacy: Report on the privacy policies and practices of health web sites, California HealthCare Foundation* (Jan. 2000), ("If a site is not careful with the design of its Web forms, data entered into a form is sent to the Web site in the query string of a URL. If the next Web page to appear contains a banner ad, then the data in the query string will be sent to the ad service company in addition to the host site." (referring to the GET method)).

[5] TIKTOK-BG-000003014; TIKTOK-BG-000009201 at -9207.

server.[6] Even once embedded, the TikTok Pixel requires additional configuration in order for advertisers to utilize its functionality.[7]

40. Advertisers can choose from 14 different "standard" events, which can be customized in addition to the ability to customize even further, through "Custom Events".[8]

41. One default event in particular, "PageView", is necessary for the TikTok Pixel to function. PageView is an indication that a website visitor has navigated to a specific page, prompting the JavaScript code to cause the browser to communicate with TTI.[9] This is how pixels work on the World Wide Web, as described *supra*.

42. The TikTok Pixel does not need to be installed on every webpage on a website because the Pixel is page-based technology.[10] Thus, it can be installed on as few specific pages as the website owner requires. In my experience, it is common to limit the pages on which pixels are installed, for many reasons. Where and how the TikTok Pixel is installed depends on the advertisers' preferences and resulting configurations of the Pixel, website code, and website configuration. In addition to my experience, Dr. Shafiq agrees that it is not the case that the TikTok Pixel must be installed on every page.[11]

43. RiteAid, one of the websites at issue in this litigation, provides a useful example of an advertiser's specific configuration of the TikTok Pixel on its website. Using Google Chrome's

---

[6] TIKTOK-BG-000003014.
[7] TIKTOK-BG-000125416 at -438.
[8] TIKTOK-BG-000002615.
[9] TIKTOK-BIG-000125480 at -81.
[10] TIKTOK-BG-000009201 at -9207.
[11] Deposition Transcript of Dr. Zubair Shafiq ("Shafiq Dep.") at 79:5-17.

Developer Tools and TikTok's Pixel Helper,[12] I was able to confirm that RiteAid's homepage, and many other pages, did have the Pixel installed. However, RiteAid's pharmacy page[13] did not have the Pixel installed.

44. The TikTok Pixel cannot cause the sending of any more information than what it is instructed by the advertiser's website to collect[14] (whether via configuration or design of the web page itself) and standard Internet protocols. Every time a user browses a website online, that user is sending data to the websites they are browsing, as well as the third parties for whom those websites decide to implement a pixel. This includes, in all cases, timestamp, IP address, user agent, URLs, and, if not blocked, cookies.

45. In addition to those data that *must* be sent because of the way the Internet and its protocols work, advertisers can choose to configure pixels to send any amount of additional data from the website visitors' browsers to third parties.[15] For example, the TikTok Pixel can be configured to send any of the values of form fields on the web page to TTI. This can be anything from details about a user's account on the advertiser's website to a customer's written complaint about a purchase. TTI calls these "properties".[16]

46. The Shafiq Report does not show any examples of "properties" data being sent to TTI. Dr. Shafiq only shows examples of data that are sent via two URLs: "URL" and

[12] TikTok Business Help Center, *Troubleshoot with Pixel Helper* (last updated May 2024), https://ads.tiktok.com/help/article/tiktok-pixel-helper-2.0?lang=en.
[13] RiteAid, https://www.riteaid.com/pharmacy (last visited July 12, 2024).
[14] TIKTOK-BG-000009201 at -9205-07.
[15] TIKTOK-BG-000125416 at -438.
[16] TikTok Business Help Center, *About Parameters* (July 2024), https://ads.tiktok.com/help/article/about-parameters?lang=en (last updated July 2024).

"Referer_URL"[17]. These URLs are already sent due to the way the Internet works, and not due to the TikTok Pixel configuration. As discussed *supra*, the parameters that are part of these URLs, based on best privacy practice by advertisers, should *not* contain the data referenced by Dr. Shafiq.

47. The cookies that the TikTok Pixel sends to TTI can only be set and read by TTI. The advertiser cannot read or set these values, and has no control over them at all. These cookies are, as discussed above, "third-party cookies", and most browsers allow consumers to choose, or sometimes by default ensure, that these cookies are *not* sent to third parties like TTI.

48. Similarly, TTI has *no* control over "first-party cookies" on the advertisers' websites. Because of the way cookies work (as described *supra*), only the domain that sets the first-party cookie can retrieve them. When the TikTok Pixel causes the user's browser to communicate with TTI, the *only* cookies that are sent are the third-party cookies, and it cannot cause first-party cookies to be sent to TTI.

49. Distinct from sending first-party cookies to another website (which cannot be done), JavaScript code such as that in pixels can cause the browser to send data to another site, outside of the cookie itself. For example, JavaScript code can read the value of a first-party cookie, and *afterwards*, cause the browser to send that datum to a third-party website as part of the URL of that website. This is described in the Shafiq Report when discussing the "_ttp" first-party cookie. However, Dr. Shafiq inaccurately describes what should be the sending of the data within this cookie as the TikTok Pixel *collecting* the cookie itself.[18] This *cookie* cannot be sent to TTI;

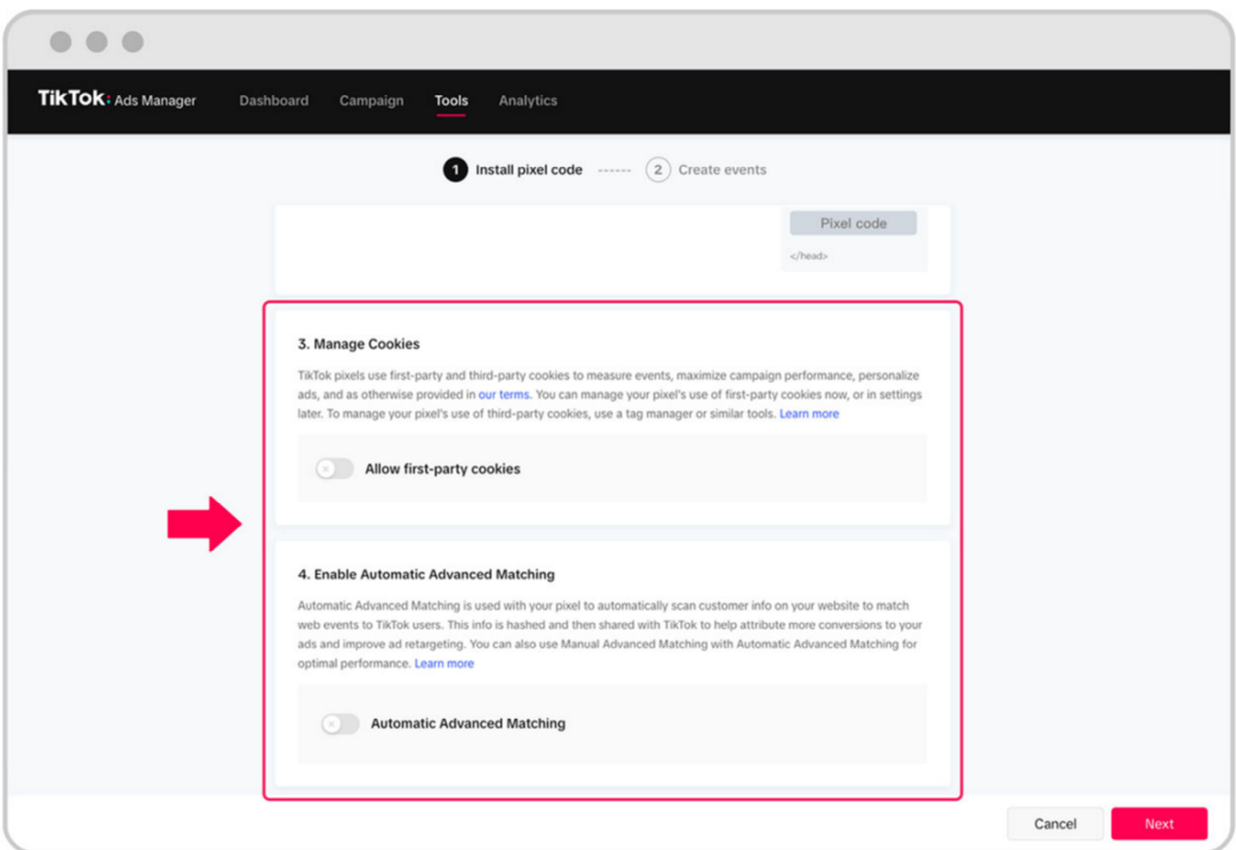
---

[17] Shafiq Report ¶ 63. The word "referrer" when used in the HTTP and URL context is misspelled "referer", due to an error in 1996 in the HTTP specification. Because of this error, almost all implementations of web servers now contain this misspelling, and it is common practice to call it by the misspelled name.
[18] Shafiq Report ¶ 62.

only the value contained within it can, which is more than pedantically different, because otherwise would suggest violating of the rules of the HTTPS protocol and the World Wide Web.

50. The _ttp first-party cookie contains a mostly random set of characters that are undecipherable. It is useful only for the purposes of matching a website visitor to an existing TikTok account holder, which I'm informed is not related to a Class in this case.

51. When an advertiser configures the TikTok Pixel for the first time, or changes the configuration later, they are presented with the option to allow or disallow first-party cookies, as shown below:[19]



[19] TIKTOK-BG-000000104 at -111.

52. If an advertiser sets this setting to **off**, no first-party cookie values will be sent from the browser to TTI when the browser sees the TikTok Pixel. This is a choice any advertiser can make and does not require any technical know-how to perform. It is part of the configuration that is performed when the TikTok Pixel is first installed, and the person configuring the Pixel will see this option as part of the configuration.[20]

53. Documentation for the TikTok Pixel describes the setting in detail, describing its importance for matching users to TikTok Account Holders when first-party cookies are enabled: "By using [first-party] cookies with Advanced Matching, you can further improve and supplement the matching of visitors on your website with people on TikTok …You can choose to not use first-party cookies with your pixel and only use third-party cookies by toggling first-party cookie usage off in your pixel settings. With this option, you will not maximize your pixel's full matching and attribution capabilities."[21]

54. [redacted][22]

55. Dr. Shafiq opines that the TikTok Pixel [redacted] However, he also states, [redacted]

[20] *Id.*
[21] TIKTOK-BG-000000236 at 239-240.
[22] Interview with Yunfeng Wei.

[redacted][23] Dr. Shafiq's assumption about [redacted]

56. My examination of the JavaScript code for the TikTok Pixel shows that [redacted] It is important to distinguish between [redacted][24] and [redacted] I also discuss *infra* the distinction between when the webpage loads, compared with when data are received by advertisers.

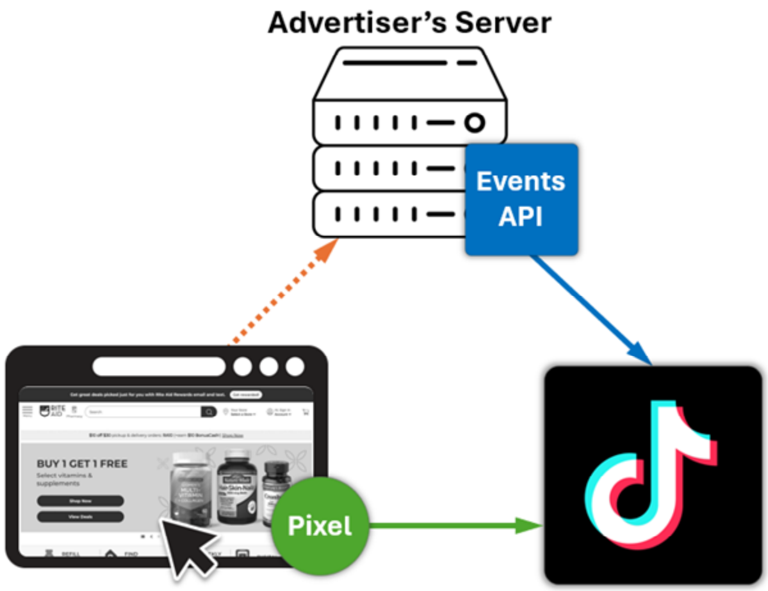
B. TikTok Events API (EAPI)

57. EAPI refers to a server-to-server connection between an advertiser and TTI. EAPI offers advertisers even more control over the sharing of information because the transmission occurs on the server-side rather than the client-side, i.e., the browser is not part of the communication.

58. This is separate from the loading of the advertiser's web page, but cannot happen until the webpage is visited, and any time after that. A separate process begins a separate communication between the advertiser and TTI, and this process can send whatever information the advertiser wants.

---

[23] Shafiq Report ¶ 32.
[24] *Id.*



59. The three main benefits of EAPI over TikTok Pixel are:

a. Advertisers have more control over what data are sent to TTI, as the data are sent directly from the advertiser to TTI. This can be configured within the default code that is available to advertisers, or code that the advertisers write themselves.

b. Server-to-Server communication is more effective at transmitting information, so there is less data loss. This is because it is not reliant on the browser or the network connection between the browser and TTI and will not be affected by user intervention such as navigating away from the page in the middle of their browsing the website.

c. It is easier to track "conversions" such as purchases or subscriptions. This is because the communication between the advertiser and TTI can happen at any time; even when the user is offline or not browsing the advertiser's website. For example, if a purchase is made over the telephone, the advertiser's back-end system can use EAPI to communicate this conversion to TTI.

60. As shown, data sent via EAPI can happen at any time, and does not have to be anywhere near the time the communication to the advertisers occurs.[25]

C. The Matching Process

61. The testimony and evidence show that the TikTok Pixel and EAPI are designed and used for optimizing the identification and understanding of TikTok Account Holders who interact with advertisements on TikTok operated by the websites that have them installed. [redacted]

[redacted]

[25] TikTok for Business Developers, *Setup Guide for Web (2024)*, https://business-api.tiktok.com/portal/docs?rid=p41a33fdhon&id=1771100865818625 (last visited July 12, 2024).

62. [redacted][26]

D. Advertisers Need to Correctly Use These Tools

63. TTI must rely on advertisers to follow best privacy practices. I am informed that advertisers who choose to use the TikTok Pixel or EAPI are required to follow TTI's applicable terms of use, including the Business Products (Data) Terms.[27] I am informed that these terms require advertisers to disclose their collection and sharing of data with third-parties and prohibit the disclosure of sensitive information.[28] Specifically, I am informed that these terms state that TTI requires advertisers using the TikTok Pixel or EAPI to provide "clear and comprehensive information to people in a sufficiently prominent notice regarding the access to, and collection, sharing, and usage of cookies."[29] In addition, TTI's terms state that "You will not share with us or enable us to access Business Products Data that you know or ought reasonably to know is from or about Children or that includes health or financial information, or other categories of sensitive information (including any information defined as sensitive or special category data under applicable laws, regulations and applicable industry guidelines)."[30]

64. Based on the documents and evidence I've examined, TTI has robust documentation to advertisers that can guide them to the proper use of these tools. They also make

[26] Defendants TikTok Inc. and ByteDance Inc.'s Amended Responses and Objections to Plaintiffs' Second Set of Interrogatories (Nos. 3-14), Amended Response to Interrogatory 6, Response to Interrogatory 8.
[27] TIKTOK-BG-000000094.
[28] *Id.* at -097, -101.
[29] TIKTOK-BG-000000236 at -041.
[30] TIKTOK-BG-000000094 at -097.

available the “Pixel Helper Tool”, which allows advertisers’ websites (and website visitors) to understand the information that is transmitted from the browser to TTI, when the TikTok Pixel is in use. When EAPI is in use, the advertiser has a direct view of what data are being sent from their own servers to TTI.

65. The TikTok Pixel is a page-specific technology and Dr. Shafiq agrees that advertisers make the choice to install the TikTok Pixel onto specific pages of their website.[31]

66. TTI could also cease to offer its advertising tools. But that would not be practical. Prohibiting the use of an essential tool to modern advertising, solely on the basis that some advertisers fail to develop their websites correctly, restricts good actors from having access to these tools. [redacted]

67. Advertisers are the only ones who can make the proper configurations to their websites and other aspects of their platform that they make available to the public. Advertisers are the ones who know their website design, obligations, and services. TTI, as a third-party, cannot control how advertisers’ websites work or how they run their businesses.

[31] See Shafiq Dep. 62:19-24 (“[redacted]”).

VII. WHETHER AND WHAT DATA ARE DISCLOSED TO TTI VIA THE TIKTOK PIXEL OR EAPI REQUIRES AN EXAMINATION OF INDIVIDUAL CIRCUMSTANCES

68. There are many factors that determine which data are transmitted to TTI by the advertisers' use of the two tools described *supra*. These factors can be different for each person who visits the advertisers' websites, as well as for each advertiser's website itself.

69. [redacted]

70. [redacted]

71. [redacted]

[redacted]

TIKTOK-BG-000118403 at D27

[redacted]

TIKTOK-BG-000118403 at D358

72. [redacted]

73. [redacted]

74. [redacted]

75. [redacted] This shows an individualized question that is by user and by advertiser.

76. [redacted]

[redacted] I also describe *supra*, and cite to scholarly articles, that this is not best privacy practice. I describe *infra*, certain issues with [redacted]

77. It is also important to note that [redacted]

78. Dr. Shafiq discusses [redacted][32] [redacted]

79. Additionally, my examination of the data showed [redacted]

80. Other variables and configurable items affect the data that are sent via these tools. These include:

a. The functionality of an advertiser's website – Some websites do not offer functionalities that allow the receipt or sharing of personal and/or sensitive data. [redacted]

[32] Shafiq Report ¶ 63(v).

b. First-party cookie settings – As described *infra*, advertisers can configure the TikTok Pixel and EAPI to not send first-party cookies. They can also restrict which first-party cookies are sent, because they have access to the JavaScript code on their own website.

c. Third-party cookie settings – Website visitors may choose to limit the sharing of information that TTI can receive through TTI's third-party cookies. In fact, as Dr. Shafiq describes, [redacted][33]

d. The website visitor's browser and ad settings – Settings and extensions can determine whether and what information is transmitted as a result of the website visitor's online activity, also described by Dr. Shafiq.[34] These tools include third-party cookie blockers, whether that be via plug-ins, extensions, or browsers themselves. Browser settings can even control which particular websites are allowed to or disallowed from placing cookies on a user's browser. There are many other privacy settings available to users, via their web browser, without knowing each user's habits, or examining their computer, it is impossible to know which of the thousands of possible permutations each user has.

e. The advertiser's website's own data privacy protocols – I am informed that TTI requires websites to obtain the necessary consents to receive visitor's information, and from my experience, I know that websites are ultimately the ones responsible and able to enforce visitor preferences.

[33] Shafiq Dep. 208:24-209:2.
[34] Zubair Shafiq, et al., *Blocking JavaScript Without Breaking the Web: An Empirical Investigation*, PETS Symposium 1, https://petsymposium.org/popets/2023/popets-2023-0087.pdf

81. [redacted]

a. [redacted][35]

b. [redacted][36]

82. [redacted]

[35] SHIH-GRIFFITH000184; SHIH-GRIFFITH000185.
[36] *Id.*

VIII. WHETHER OR NOT SEARCH TERMS OR ANY WEBSITE USER COMMUNICATIONS WERE COLLECTED IS AN INDIVIDUALIZED QUESTION

83. Dr. Shafiq discusses seven pieces of data that are "always" sent to TTI when the TikTok Pixel is installed: Timestamp, IP Address, User Agent, Cookies, URL, Event Information, and Content Information.[37] Some of these are automatically sent to any website, as discussed *supra*. All of these are different, depending on both the users and the advertisers' websites.

84. Dr. Shafiq's premise starts with the presumption that [redacted]

85. Dr. Shafiq claims that [redacted][38] I disagree with that statement for two reasons: [redacted]

[37] Shafiq Report ¶ 83.
[38] *Id.* ¶ 84.

86. [redacted]

87. [redacted]

88. [redacted]

89. [redacted]

90. Below, I discuss other important aspects of the seven categories.

a. **Timestamp.** Under the circumstance that the TikTok Pixel sends data to TTI at close to the same time as the page is loaded, the timestamp is certainly independently derivable by TTI. TTI needs only to look at its own timeclock to see what time it is. But indeed

the TikTok Pixel JavaScript code causes the browser to send an independent timestamp as part of the communication. This allows TTI to see what time the event actually happened, in the case that it may be a different time than the communication. As I discuss *supra*, [redacted]

b. **IP Address.** Unlike the timestamp category, [redacted]

c. **User Agent.** [redacted]

d. **Cookies.** I discuss Cookies at length, *supra*. [redacted]

e. **URL.** I discuss URLs at length, *supra*. [redacted]

f. **Event Information.** As discussed *supra*, [redacted][39] However, it is completely customizable by the advertiser. In fact, I found [redacted]

g. **Content Information.** By definition, the content information is completely different for each webpage that results in the TikTok Pixel or EAPI being used. Dr. Shafiq states, [redacted][40] He goes on to explain how "[redacted]

[39] Shafiq Report ¶ 64.
[40] *Id.* ¶ 65.

[redacted][41] [redacted]

91. In Dr. Shafiq's deposition, he conceded that [redacted][42]

92. However, this completely ignores the fact that if best privacy practices were used by the advertiser, [redacted] By using the POST method of passing parameters, as I describe *supra*, [redacted] It is not only when the website has no search functionality.

93. [redacted]

IX. WHETHER [redacted] OR SENSITIVE INFORMATION WAS DISCLOSED IS AN INDIVIDUALIZED QUESTION

94. Dr. Shafiq states that [redacted][43]

---

[41] *Id.*
[42] Shafiq Dep. 137:3-11.
[43] Shafiq Report ¶ 63(v) & fn.214.

95. I do not have an opinion on what [redacted] is, from the legal sense, so I cannot rebut him in terms of whether or not [redacted] However, I do have some opinions on [redacted]

96. Dr. Shafiq is specifically talking about "[redacted]".

97. It is important to note that [redacted]

98. [redacted]

99. As I discuss *supra*, i[redacted]

100. Dr. Shafiq detailed several ways in which website owners can—and do, according to best practice—[redacted]"[44]

[44] Shafiq Dep. 50:24-25, [redacted]

101. Dr. Shafiq also answers some questions about the GET method versus the POST method. When asked, [redacted][45] He continues, when asked, [redacted][46]

102. These responses indicate that Dr. Shafiq is not answering the question in terms of the topic at hand. The inquirer is asking about [redacted] Based on my reading of Dr. Shafiq's prior research, he understands that putting parameters in POST data as opposed to using GET will ensure that those data are not seen in the URL that is passed via the JavaScript that is used in the TikTok Pixel.[47]

103. While it is true that "POST requests have URLs", the distinguishing feature between GET requests and POST requests is that the parameters can be in the payload of the

[45] Shafiq Dep. 56:23-57:4.
[46] *Id.* at 57:5-11.
[47] Yash Vekera, et al., *The Inventory is Dark and Full of Misinformation: Understanding Ad Inventory Pooling in the Ad-Tech Supply Chain*, 45th IEEE Symposium on Security and Privacy (SP) (2024), https://web.cs.ucdavis.edu/~zubair/files/Programmatic-IO-DarkPooling.pdf ("We extracted the URLs, content, and HTTP POST-encoded data from each ad-related request and response.");
Shaoor Munir, et al., *PURL: Safe and Effective Sanitization of Link Decoration* n.18 (Aug. 2023), https://arxiv.org/abs/2308.03417 (citing to code used to query parameters from URLs that only checks for parameters if the request is using GET, rather than POST).

message, as opposed to being part of that URL. It is also true that an HTTPS message with a POST request *can* have parameters in the URL, but that would be problematic because, 1) It defeats the purpose of using a POST request, other than if you for some reason want certain parameters to be in the URL and certain (probably sensitive) parameters to not be in the URL, and 2) The way websites are written, one usually needs to know whether to expect parameters to be in the URL, or in the payload. The code on the website would need to look at both, if it's not sure where they are supposed to be, or if it expects it to be in both. This is inefficient, and over millions and millions of requests, inefficiencies add up.

104. More importantly, the GET vs POST decision by the advertisers is unrelated to whether or not the POST method can contain parameters in the URL. The question is whether or not, if the advertisers pass parameters from one webpage on their website to another using the POST method, will these parameters be invisible to TTI when the TikTok Pixel sends the URL, and the answer is yes.

105. Another method of passing parameters within the URL if the GET method must be used for some reason, is to *encrypt* the parameters within the URL.[48] Using a cipher that only needs to be known by the website, the parameters can be completely opaque to any other website that ends up receiving them, whether that be due to a pixel, or due to other navigation from the website. I have personally done this when necessary to use the GET method.

[48] Shaoor Munir, et al, PURL: Safe and Effective Sanitization of Link Decoration (2023), https://arxiv.org/abs/2308.03417 ("This approach has been attempted by Facebook [94] to circumvent query parameter stripping. In Facebook's case, the obfuscated URL (e.g., https://www.facebook.com/user/posts/pfbid0RjTS7KpBA...) contains a single encrypted resource path that essentially combines multiple query parameters.")

106. In terms of the [redacted][49] [redacted][50]

107. I found it notable that [redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

108. [redacted]

109. [redacted]

[49] Shafiq Report ¶ 63(v).
[50] *Id.*

[redacted]

110. [redacted]

X. WHETHER COMMUNICATIONS BY THE WEBSITE VISITOR ARE COLLECTED WHILE "IN TRANSIT" TO THE WEBSITE REQUIRES AN EXAMINATION OF INDIVIDUAL CIRCUMSTANCES

111. I was asked by counsel to examine whether or not there is an interception of the contents of communications while those communications are "in transit". I understand "contents of a communication" are more akin to data such as a website visitor's search queries or personally identifiable information, and not akin to some of the data I've described in my report so far, such as timestamp or a URL that does not reveal a communication. The "in transit" component implies a timing question, which I understand asks whether the communication is intercepted simultaneously to its transmission. I used my technology experience to evaluate this issue.

112. From a computer science standpoint, contents of a communication that are sent to a third party after the information is done being received by a website's server would not be considered to be "in transit" any longer.

113. Determining whether or not advertisers disclose browsing information to TTI via the TikTok Pixel while "in transit" requires a case-by-case look at the data being collected, as well as how the advertiser's website has configured the TikTok Pixel.

A. TikTok Pixel Timing

114. The **event parameters** that advertisers configure for the TikTok Pixel on particular web pages on their website ultimately determine what data are shared with TTI. To illustrate, a website visitor who clicks on an "Add to Cart" button can trigger a different response from the TikTok Pixel than is the case for a visitor executing a "Search Function".

115. For "Add to Cart", the website may prevent navigation to a new webpage by simply adding it to the cart without changing the user interface (other than changing a quantity number on a picture of a shopping cart, for example), or it may open a completely new page automatically that shows the complete cart listing. This is a decision that the advertiser needs to make. For "Search", the website usually navigates the user to an entirely new web page containing search listings.

116. For each of these cases where a new webpage is opened, typically the URL collected by the TikTok Pixel will look different than the page before it. In some cases, the website may share data in the form of a URL as a "referrer page", which contains the name of a previous webpage that the visitor visited.

117. The data from a referrer header, by definition, concerns communications from a website visitor to a website they already visited in the past. This communication, also by definition, already occurred by the time data about that visit are shared with TTI, i.e., by the time

the TikTok Pixel is capable of sending the referer_URL, the user has already left the page that URL describes (including any parameters that might be in that URL).

118. If we are discussing timing, there can be no question that any data in the referer_URL, by definition, are data that were sent to and received by the website's servers previously to the "current" webpage (the one with the TikTok Pixel).

119. Dr. Shafiq admits that [redacted] He states, "[redacted]"[51] Dr. Shafiq is [redacted][52]

120. The Shafiq Report focuses on the "PageView" event, which he believes is consistently transmitted to TTI across *all* web pages within a website. When asked [redacted]"[53] [redacted]

[51] Shafiq Dep. 161:10-12.
[52] *See*, *e.g.*, Shafiq Dep. 165:1-3, 165:22-166:1, and 167:10-12.
[53] Shafiq Dep. 109:3-6.

[redacted]"[54] and continued, "[redacted]"[55]

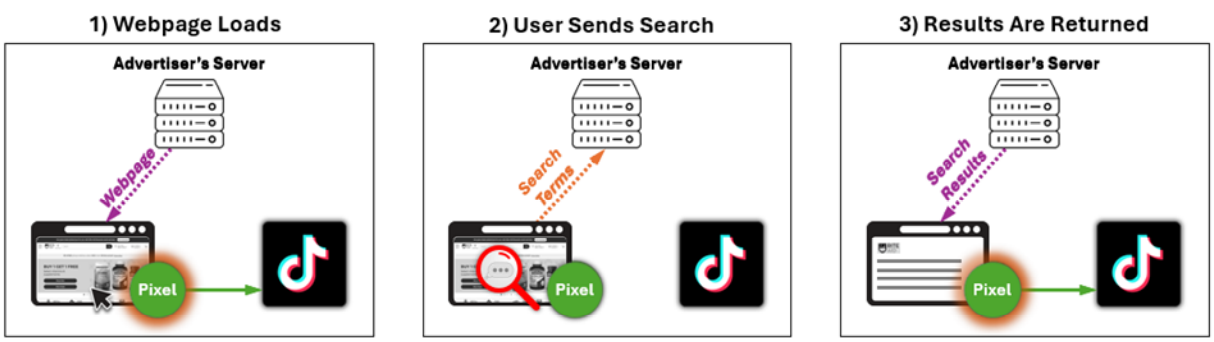
121. [redacted]

122. In terms of the timing of when messages are transmitted for web pages that *do* have the TikTok Pixel installed, this requires some technical background explanation. To describe what happens when a web page different from the previous webpage is loaded, it is important to know that there are several components to web traffic on the Internet. The Browser runs on the visitor's computer. This computer is connected to the Internet. It transmits packets to the server computer that is *hosting* the webpage.[56] The data contained in these packets, which in the examples we've been discussing include web parameters and other data, are said to be going "over the wire" (even if some of it is technically wireless). When the packet is received by the host of the website, it is first processed by the network hardware, and then the network layer of the Operating System (typically Linux). The Operating System then decides where to send these data. In this case, it will be sent to software on the computer that is known as the web server.[57] Note that at this point, all of the "over the wire" activity from the browser to the web server has been completed. Once the web server software receives the packets, it decides what webpage to load and send back to the remote computer (the visitor's computer). Once the response is received by the visitor's computer, the visitor's browser can load and render the page. If that page has a TikTok Pixel on it, it will

[54] Shafiq Dep. 109:7-12.
[55] Shafiq Dep. 110:14-15.
[56] There are usually intermediary computers that make up the "backbone" of the Internet, but I leave these out for brevity.
[57] Two examples of the most often-used web server, in my experience, are Apache and Nginx.

begin a communication with TTI (unless one of the visitor's extensions or ad blockers prohibits that).

123. It is important to note that by the time the data that are sent to the new web page are sent to TTI, the website's host server has *already* received the transmission (in total) from the browser. This is true even if, as Dr. Shafiq describes, [redacted]".[58] [redacted]



B. EAPI Timing

124. Through EAPI, TTI's server can only receive data from an advertiser's server after the advertiser has already collected information onto not only its host server as described *supra* relating to the TikTok Pixel, but also has been completely received by the web server software. In other words, TTI cannot receive information about a user's interactions with the advertiser's platform in real-time. The advertiser must first collect that information onto its web server and then choose to share it with TTI's servers. Dr. Shafiq states, [redacted]

[58] Shafiq Report ¶ 10.

[redacted][59]

125. Dr. Shafiq's [redacted]"[60] When evaluating the timing of when Internet transmissions occur, it is important to be precise. TTI's use of the words "as soon as it is seen", communicates the fact that it must *first* be "seen" on the advertiser's server. This is an important piece of information for evaluating timing.

126. Additionally, many of the use cases of EAPI, such as "conversions" as I describe *supra*, actually *require* that the data be sent via EAPI hours, days or even longer after the data have been received by the advertiser.

XI. COMPARISON OF DATA COLLECTED THROUGH GOOGLE IPSOS SCREENWISE OR SAVVYCONNECT VERSUS TIKTOK PIXEL REQUIRES INDIVIDUALIZED ANALYSIS

127. Dr. Shafiq opines, based on available public disclosures, "that the data collected by Google [Ipsos] appears comparable to the default categories of data collected by the TikTok Pixel."[61]

---

[59] Shafiq Dep. 125:5-21.
[60] Shafiq Report ¶ 41.
[61] Shafiq Report ¶¶ 83-85 (at pp. 59-60).

128. Dr. Mangum concludes, also based on available public disclosures, that "…the market value of the Class Member data collected by the TikTok SDK is most consistent [sic] and economically comparable with the SavvyConnect and Screenwise programs."[62]

129. Dr. Shafiq reaches his conclusion based on the Google Panel Privacy Policy, in which he says data collected by Ipsos "may include every web page visited and all interactions (e.g., mouse clicks) with those webpages, including URL and IP address and the length of time you spent visiting websites; data about the browser used by panelist and his or her browser settings, and cookies."[63]

130. In order to do a proper comparison with Ipsos, you must look at what is compared. This is what the Google Panel Privacy Policy discloses Ipsos collects:

- "Use of Your Devices," which "potentially will collect and record all interactions with that device" including a participant's mobile phone. Ipsos may collect "Content and Advertising" including internet activity, apps and operating systems, telephone, emails, SMS, instant messaging, and other "communications services", digital media, TV, game consoles, and other shared devices, clicks and taps, audio data, "information you provide", content on the screen, and local storage information (including personal information).

- Cookies.

[62] Mangum Report ¶ 113.
[63] Shafiq Report ¶ 84 (at p. 60).

- Device Information, including device identification, location information, sensors, system status and data usage, and network and connectivity information.

- Diagnostic and Device Data.

- Smart Devices.

131. Dr. Shafiq does not explain how "[t]hese categories are substantially similar to the seven data categories collected by TikTok Pixel…[including] URL, IP Address, Timestamp, User Agent (which identifies website visitor's [sic] operating system, vendor, browser, and browser version), and Cookies."[64]

132. A simple comparison shows the biggest difference between the two is that Google Ipsos collects *all* of the panelists' Internet activity. This is not even limited to websites. Savvyconnect collects *all* of the panelists' web browsing. TikTok Pixel is only collecting information that only TTI's advertisers decide to send to TTI. This is *only* on websites and the web pages on those websites on which advertisers decide to install the TikTok Pixel.

133. Another significant difference is that Ipsos can collect information on *all* of a user's devices and what those devices do over the Internet. This is because a part of their functionality is to send panelists a specialized router that has unlimited access to what the panelists are doing on the Internet.

134. Google Ipsos is orders of magnitude more comprehensive about its collection of data about a pre-identified individual's interactions across all devices, platforms, apps, websites,

---

[64] Shafiq Report ¶ 85 (at p. 60).

and other Internet access, including a participant's personal audio communications with another. SavvyConnect collects data for unlimited websites browsed by the panelists. Dr. Shafiq does not explain why anyone would pay the same or any more than a fraction of the amount of money for the seven categories of data that he claims are always collected by the TikTok Pixel, and limited to the websites that are advertisers for TTI.

135. For both Ipsos and SavvyConnect, another difference is that it is easy for those companies to tie the data to a particular person because the data are collected all at once to a *registered* user of those services. Here, instead, TTI sometimes gets snippets of data in different times, different ways, and in a manner that could not be used to reliably isolate and compile data on individual events into a browsing history for a non-TikTok user or attribute that history to a non-TikTok user ([redacted]).[65]

I declare under the penalty of perjury that the foregoing information is true and correct. Executed this 12th day of July, 2024 in Miami, Florida.

Ron Schnell

12 July 2024

[65] Defendants TikTok Inc. and ByteDance Inc.'s Amended Responses and Objections to Plaintiffs' Second Set of Interrogatories (Nos. 3-14), Amended Response to Interrogatory 6, Response to Interrogatory 8.

Ron Schnell

1111 Brickell Ave, Suite 2050, Miami, FL 33131
Mobile (954) 682-7822 – rschnell@thinkbrg.com

Executive Profile

Accomplished executive with a history of running large technology organizations, from early stage startups to large divisions of S&P 500 corporations. Strategic consultant and forward-thinking technology and architecture expert, with a unique understanding of the low-level "bits" (as a former kernel programmer) as well as the business rules and implications. Successful at managing diverse engineers and stakeholders, while digging in and writing code where necessary.

40+ years of experience in technology, 30+ years of executive experience, 40+ years of experience in Artificial Intelligence. Founder of 3 startups, one with exit to a public company. Early architect of UNIX kernel. Special Master experience and Monitorship experience. Knowledge and coding experience of most computer languages, including many assembly languages.

Technical Expertise

- Artificial Intelligence/Machine Learning
- Advertising/Tracking Pixels
- BIPA/VPPA
- Source Code Analysis
- Software Project Management/Remediation/Analysis
- Blockchain (Private/Public)
- OS Kernel
- Device Drivers
- Very Large Database Architecture and Analysis
- Healthcare Software
- Autonomous Driving Software
- Breach Investigation/Remediation
- Forensic Analysis
- Bid Protest Analysis
- Patent Analysis (IPR/District Court)

Professional Experience

Managing Director
September 2013 – Present
Berkeley Research Group

Testifying and consulting expert in highly-technical litigation and large-scale corporate and board level consulting. Gives testimony in Federal Court, State Court, Depositions and Arbitrations. Writes expert reports as an independent expert for litigation. Technical advisory

consulting work for all types of companies and boards of directors. Litigation support includes source code reviews in many languages, architecture review, and advice on software trade secret and copyright issues.

President
February 2005 – Present
Quogic, Inc. – Ft. Lauderdale, FL

Perform per-project consulting for corporate clients, which have included:
Intel Corporation (via Berkeley Research Group) **–** Board/executive level strategic consulting
AEther, LLC – Inflight entertainment system architecture and development
Virgin America Airlines – Inflight entertainment system architecture
BidKind, LLC – Charity auction site architecture and development management
HockeyTech, Inc. – Sports management software architecture and development
Several law firms as testifying and consulting expert witness

Adjunct Professor of Computer Science, Board Member: Graduate School of Computer Science
August 2013 – Present
Nova Southeastern University, Ft. Lauderdale, FL

Classes in Cyber Security and Operating Systems

President
August 2012 to August 2013
Invenstar, LLC – Boca Raton, FL

Ran day-to-day operations of hardware and software manufacturing company in the point-of-sale space for retail establishments. Architected cloud-based point-of-sale system and managed all developers.

General Manager - Chief Executive
May 2005 to August 2011
Technical Committee – Bellevue, WA and Palo Alto, CA

Ran day-to-day operations (as chief executive) of private corporation ordered to be formed by the United States Courts. This corporation was tasked with monitoring Microsoft Corp., ensuring their compliance with the Final Judgments in the US v. Microsoft/NY v. Microsoft antitrust case filed in 1998. Daily interaction with Microsoft executive and senior staff, Microsoft competitors and partners, Attorneys General/Deputies for multiple states, Assistant Attorneys General for the United States, and representatives from other countries. Was responsible for responding to potential complaints from 3rd parties. Hired over 90 people to work in 3 offices.

Vice President
April 2002 to January 2005
Equifax Corporation – Boca Raton, FL

Head of software development, network relations, privacy and data security, new product development, and data enhancement delivery technology for the Internet Marketing division of Equifax, at the time a 105-year-old company. Was responsible for architecting software products, B-to-B processes, and assigning personnel. Responsible for long-term planning for

strategy and expenditures. Interfaced with key people at vendors, clients, and service providers. Oversaw integration of major corporate acquisitions, creating efficiencies in technologies and personnel. Created partnerships and was liaison with companies including AOL, Yahoo, and Microsoft. Headed team that coordinated data enhancement of client databases, and delivered enhanced data to those clients. Implemented processes, quality controls, project planning and client interfaces by technical staff. Chairperson of committee that made decisions on types of marketing accepted, approval for types of clients/messages, and responses to complaints. Performed integration of several acquired companies, including technical integration as well as integration of staff and other efficiencies of scale. Spoke on behalf of Equifax at the Federal Trade Commission (FTC) on *spam* and anti-spam technology.

Senior Vice President, Chief Technology Officer
February 2000 to February 2002
Voice and Wireless Corp – Minneapolis, MN

Responsible for all technology decisions for the public company that acquired Mail Call, Inc. in 2000. Made product decisions, architected product enhancements, and recommended technology direction. Oversaw acquisitions of other technology companies. Participated in due diligence for potential acquisitions, and interfaced with other potential buyers of technology. Spoke at shareholder meetings and other shareholder events.

Founder, President, Chief Technology Officer
May 1997 to February 2002
Mail Call, Inc. – Pembroke Pines, FL

Founder of corporation providing a service to business consumers, allowing them to retrieve and manage their E-Mail over the phone. Performed project design, project management, data privacy and security, all software programming and testing. Negotiated contracts with all partners, including GTE, Verizon, Concentric Networks, Net2Phone, IDT, Earthlink, Casio, Knight-Ridder, T-Mobile (Voicestream) and others. Managed all staff. Implemented exit strategy by negotiating buyout by Voice and Wireless Corp.

President
February 1994 to January 2003
Driver Aces, Inc –Miami, FL

President of corporation specializing in developing device drivers for the UNIX operating system. Performed project design, project management, driver design, driver authoring, driver testing, customer contact, sales, and staff management. Customers included Sun Microsystems, IBM, Digital Equipment, SCO, Lucent Technologies, and others. Drivers were for high-speed networking devices, including fast Ethernet, token-ring, and fiber-optic, SCSI devices, RAID controllers, serial devices, parallel devices, and pseudo-devices. Managed staff of developers.

Consultant - Kernel Programmer
January 1992 to June 1995
Sun Microsystems – Los Angeles, CA

Worked in the Peripherals Engineering group, Multiprocessor group, and Device Driver group. Was responsible for various programming and testing on Solaris 2.1, 2.4, 2.5, and 2.5.1. Wrote kernel and driver code for Solaris x86, Sparc, and PowerPC. Performed bug-fixing, authoring of

system software, kernel enhancement, and device driver authoring for high-performance network and serial drivers. Was responsible for development of device driver porting kit. Wrote a book entitled Solaris 2.1 Guide to Porting SVR4.0 Device Drivers for x86. Worked with Independent Hardware Vendors on getting device drivers ported to Solaris. Re-wrote existing network drivers to improve network performance and to add multiprocessor/multithreaded functionality.

Principal Member of Technical Staff
September 1991 to December 1992
Encore Computer Corp. – Ft. Lauderdale, FL

Worked on new massively parallel hardware, developing UMAX V in the kernel development group. Developed device drivers for new memory cards, fixed kernel bugs, worked in a team implementing RPC system, and worked on tcp/ip network code for use on a proprietary network.

Founder, President
March 1990 to June 1991
Secure Online Systems, Inc. – Los Angeles, CA

President and founder of a software company that developed and marketed system management software for UNIX, specializing in data security. Designed packages, then managed development project. Investigated strategic relationships in order to create channels of distribution. Managed office staff including programming and marketing. Designed and oversaw creation of product brochures. Wrote new device drivers, kernel modifications, applications in X-windows including Motif, TCP/IP applications, database applications, and screen management routines.

Consultant - Development manager and kernel programmer
September 1988 to February 1990
IBM Corp. – Los Angeles, CA

Worked on AIX/370 and AIX PS/2. Was site lead architect and made many design decisions affecting the end product. Worked on kernel, commands, customer support, and applications. Supervised 15 programmers and testers who reported directly to me. Implemented new device drivers, fixed many bugs, made changes to TCP/IP layer, hired new employees, made OS POSIX compliant, and taught several classes. Also worked on internals of TCF (transparent computing facility) on site at Locus Computing Corporation.

Consultant - Kernel Programmer
May 1987 to September 1988
AT&T Bell Laboratories – Summit, NJ

Worked on the UNIX project, developing UNIX System V release 4.0, in kernel development group. Developed new "filesystem independent boot" feature and a new filesystem type; fixed performance, security, and fault types of bugs in UNIX kernel; wrote a new hard disk device driver; oversaw software development contracted out to remote sites; acted as a mentor to new employees; was part of the design and architecture teams dealing with firmware and machine diagnostics; and interacted directly with Sun Microsystems on joint software development.

Academia and Education

Syracuse University	Master of Science, Computer Science
Nova Southeastern University	Adjunct Professor of CS (present)
	Board, Graduate School of CS (past)
YPO Palm Beach	Education Chair, Vice Chapter Chair (past)
YPO Southeast US and Caribbean Region	Education Chair (past)

Personal Information

- Instrument rated pilot for 35 years; donates pilot time and aircraft to Angel Flight
- Arbitrator since 2000 for the state of Florida, hearing and deciding cases several times a month, usually for the Lemon Law
- Wrote freeware text adventure game that ships with all modern versions of the UNIX Operating System, including Mac OS
- Captain – US Polo Bears – International Segway Polo Team

Ron Schnell

EXPERT EXPERIENCE (TESTIMONY ONLY)

*Openrisk, LLC v. **Microstrategy Services Corporation** (**Robbins, Russell, Englert, Orseck, Untereiner & Sauber**) 1:15-cv-01451 (Eastern District of Virginia) (Misappropriation of trade secret/Copyright Infringement)

*Openrisk, LLC v. **Microstrategy Services Corporation** (**Robbins, Russell, Englert, Orseck, Untereiner & Sauber**) 1:14-cv-01244 (Eastern District of Virginia) (Misappropriation of trade secret/Copyright Infringement)

*Cincinnati Insurance Company v **Actuate Corporation** (**Tucker Ellis LLP**) 1:12-cv-00338 (Southern District of Ohio) (Software licensing)

†**Opal Labs Inc.** (**Markowitz Herbold PC**) v. Sprinklr, Inc. et al 3:18-cv-01192 (Oregon) (Misappropriation of Trade Secret)

†Shirmel Gumbs-Heyliger v. **Military Personnel Services, Corp**. (**Sanford Amerling & Associates**) 1:12-cv-00078 (US Virgin Islands) (Wrongful termination)

†United States of America v. **Sinovel Wind Group Co., LTD, Su Liying, Zhao Haichun, and Dejan Karabasevic** (**Alston & Bird**) 3:2013-cr-00084 (Wisconsin) (Theft of trade secret, Economic Espionage)

†**Kim Peter Tillman** (**Gunster**) v. Advanced Public Safety, Inc. and Trimble Navigation Limited 9:2015-81782 (Southern District of Florida) (Software - Whistleblower Act)

†**Couple Up Plus LLC** (**Astigarraga Davis**) v. SDSOL Technlogies, LLC. AAA Case No. 01-14-0001-3682 (Software contract breach)

*Sigma 3 et. al v. Ouenes et. al (**Retained directly by the Arbitrator, Judge Susan Sousson)** AAA Case No. 01-16-0005-4951 (Misappropriation of Trade Secret)

***Advanced Dentistry of Plantation, P.A.** (**Schulman Law Group**) v. Brown & Brown of Florida, Inc. CACE15007317 (05) 17th Judicial Circuit, Broward County, FL (Insurance - cause of loss - computer failure)

†Oracle America, Inc. et al. v. **Hewlett Packard Enterprise Company** (**Gibson, Dunn & Crutcher**) 3:16-cv-01393 (Northern District of California) (Copyright Infringement)

†**Nuance Communications, Inc** (**Weil, Gotshal & Manges)** v. IBM Corporation 7:16-cv-05173 (Southern District of New York) (Software licensing)

*Google, Inc. v. **Spring Ventures, Ltd.** (**Meister Seelig & Fein**) IPR2017-01653 (Inter Partes Review) (Patent Infringement)

*Gates Corporation v. **CRP Industries, Inc.** (**McCARTER & ENGLISH, LLP**) 1:16-cv-01145 (District of Colorado) (Misappropriation of Trade Secret)

†Michael Reed v. **SBM Site Management (Seyfarth Shaw, LLP)** AAA Case No. 01-18-0002-0952 (Breach of Contract)

*Dolby Laboratories Licensing Corporation et al v. **Adobe Inc. (Arnold & Porter)** 4:18-cv-01553 (Northern District of California) (Copyright Infringement)

*M-I L.L.C v. **Q'Max Solutions, Inc. et al (BoyarMiller)** 4:2018-cv-01099 (Southern District of Texas) (Misappropriation of Trade Secret)

***Aon PLC et al (Littler Mendelson)** v. Infinite Equity, Inc. et al 1:19-cv-07504 (Northern District of Illinois) (Misappropriation of Trade Secret)

*TPI Cloud Hosting, Inc. v. **Keller Williams Realty, Inc. (Norton Rose Fulbright)** 1:19-cv-808 (Western District of Texas) (Misappropriation of Trade Secret)

*Vanderbilt University v. **Scholastic, Inc. et al (Weil, Gotshal & Manges, Frankfurt, Kurnit, Klein & Selz, P.C., Neal & Harwell, PLC)** 3:18-cv-00046 (Middle District of Tennessee) (Breach of Contract)

†4DD Holdings et al v. **United States of America** 15-945C (Court of Federal Claims) (Software License)

†Calsep, Inc. v. **Ashish Dabral et al (Boyar Miller)** 4:19-cv-01118 (Southern District of Texas) (Misappropriation of Trade Secret)

***HumanTouch, LLC (Ward & Berry)** v. United States of America 16-561C (Court of Federal Claims) (Breach of Contract)

*Paycargo, LLC v. CargoSprint, LLC et al **(Appointed as Special Master)** 20-cv-22885, (Southern District of Florida) (Misappropriation of Trade Secret)

***MedImpact Healthcare Systems, Inc. (Jones Day)** v. IQVIA, Inc. 3:19-cv-01865, (Southern District of California) (Misappropriation of Trade Secret)

*****Better Holdco, Inc. (Friedman Kaplan)** v. Beeline Loans, Inc. 1:20-cv-08686 (Southern District of California) (Misappropriation of Trade Secret)

†John C. Depp, II v. **Amber Laura Heard (Charlson Bredehoft Cohen & Brown, P.C.)** CL-2019-2911 (Circuit Court of Fairfax County, Virginia) (Defamation of Character)

*Broadband iTV, Inc. v. **Orrick Herrington & Sutcliffe, LLP et al (Long & Levit LLP)** 21STCV16407 (Superior Court of California, County of Los Angeles) (Breach of Fiduciary Duty and Negligence)

*****Ruben A. Luna et al (Robbins Geller Rudman & Dowd)** v. Carbonite, Inc. et al 19-cv-11662 (District of Massachusetts) (Shareholder Derivative)

*OSGHC, LLC v. **Nomi Health, Inc. (Baker Botts) DC-22-03963** (District Court, Dallas County, TX) (Breach of Contract)

*****Webroot, Inc., et al (King & Spalding)** v. AO Kaspersky Lab, et al 6:22-cv-00243 (Western District of Texas) (Patent Infringement)

†ISIS Solutions, Inc. v. **Aurora Predictions, LLC (Fortis Law)** 1200055354 (JAMS Arbitration) (Misappropriation of Trade Secret)

*Everett Bloom et al v. **Zuffa, LLC et al (Paul Hastings)** 2:22-cv-00412 (District of Nevada) (Video Privacy Protection Act)

---

* Testified at deposition
†Testified at trial, evidentiary hearing, or live arbitration

Appendix C - Materials Relied Upon by Ron Schnell

Pleadings
Second Amended Class Action Complaint, filed April 11, 2024 (ECF No. 137)
Plaintiffs' Memorandum of Points and Authorities in Support of Their Motion for Class Certification, filed June 21, 2024 (ECF No. 179-1)
Joint Stipulation re Motion to Compel Production of Source Code (revised), filed April 4, 2024 (ECF No. 127)
Declaration of Christopher J. Lee In Support of Plaintiffs' Motion to Compel Production of Current And Historical Source Code, filed Aril 4, 2024 (ECF No. 127-1)
Discovery Documents
TikTok Inc. and ByteDance Inc.'s Amended Responses and Objections to Plaintiffs' Second Set of Interrogatories (Nos. 3-14)
TikTok Inc. and ByteDance Inc.'s Amended Response and Objections to Plaintiffs' Interrogatory 6
TikTok Inc. and ByteDance Inc.'s Response and Objections to Plaintiffs' to Interrogatory 8
Deposition Testimony
Deposition Transcript of Jacob Leady (06/25/2024)
Deposition Transcript of Bernadine Griffith (06/26/2024)
Deposition Transcript of Patricia Shih Blough (06/27/2024)
Deposition Transcript of Dr. Zubair Shafiq (07/02/2024)
Expert Reports (Including Backup Materials)
Declaration of Russell W. Mangum III, Ph.D., in Support of Plaintiff's Motion for Class Certification (06/21/2024)
Declaration of Zubair Shafiq, Ph.D., in Support of Plaintiffs' Motion for Class Certification (06/21/2024)
Interviews
Yunfeng Wei

Bates Stamped Documents
SHIH-GRIFFITH000184
SHIH-GRIFFITH000185
TIKTOK-BG-000000094
TIKTOK-BG-000000104
TIKTOK-BG-000000158
TIKTOK-BG-000000236
TIKTOK-BG-000000274
TIKTOK-BG-000000279
TIKTOK-BG-000000365
TIKTOK-BG-000000386
TIKTOK-BG-000000412
TIKTOK-BG-000000835
TIKTOK-BG-000000853
TIKTOK-BG-000002273
TIKTOK-BG-000002615
TIKTOK-BG-000002788
TIKTOK-BG-000002789
TIKTOK-BG-000002855
TIKTOK-BG-000002930
TIKTOK-BG-000002941
TIKTOK-BG-000002983
TIKTOK-BG-000003014
TIKTOK-BG-000003045
TIKTOK-BG-000003193
TIKTOK-BG-000003218
TIKTOK-BG-000008114
TIKTOK-BG-000008616
TIKTOK-BG-000009201
TIKTOK-BG-000009209
TIKTOK-BG-000009378
TIKTOK-BG-000009604
TIKTOK-BG-000009777
TIKTOK-BG-000009786
TIKTOK-BG-000118403
TIKTOK-BG-000124043
TIKTOK-BG-000125283
TIKTOK-BG-000125416

TIKTOK-BG-000125480
TIKTOK-BG-000125520
TIKTOK-BG-000125913
TIKTOK-BG-000168039
TIKTOK-BG-000168075
TIKTOK-BG-000168298
TIKTOK-BG-000168709
TIKTOK-BG-000179577
Articles/Industry Reports/Websites
Janlori Goldman, , Zoe Hudson, and Richard M. Smith, *Privacy: Report on the privacy policies and practices of health web sites. Oakland, CA: California HealthCare Fundation* (Jan. 2000)
Jay L. Himes, Jason Nieh & Ron Schnell, *Antitrust Enforcement and Big Tech: After the Remedy Is Ordered*, 1 Stanford Computational Antitrust 64 (2021)
Kevin Beaver, *Why use POST vs. GET to keep applications secure*, TechTarget (Feb. 9, 2010), https://www.techtarget.com/searchsoftwarequality/tip/Why-use-POST-vs-GET-to-keep-applications-secure
Ron Schnell, *Hacking 101: Using Social Engineering Increases Security Attack Effectiveness*, Coast Guard J. of Safety & Sec. at Sea, Procs. of the Marine Safety & Sec. Council 71, no. 4 (2014) 25–27
Shaoor Munir, et al, *PURL: Safe and Effective Sanitization of Link Decoration*, (citation 18) (Aug. 2023)
TikTok Business Help Center, About Parameters, TikTok *available at* https://ads.tiktok.com/help/article/about-parameters?lang=en (last updated July 2024)
TikTok for Business Developers, *Setup guide for Web* (2024), https://business-api.tiktok.com/portal/docs?rid=p41a33fdhon&id=1771100865818625)
TikTok Business Help Center, *Troubleshoot with Pixel Helper* (2024), https://ads.tiktok.com/help/article/tiktok-pixel-helper-2.0?lang=en
W3Schools, *HTTP Request Methods* (2024), https://www.w3schools.com/tags/ref_httpmethods.asp
Yash Vekera, et al, *The Inventory is Dark and Full of Misinformation: Understanding Ad Inventory Pooling in the Ad-Tech Supply Chain*, 45th IEEE Symposium on Security and Privacy (SP) (2024)
Zubair Shafiq, et al, *Blocking Javascript Without Breaking the Web: An Empirical Investigation*